ABSTRACT

An circuit arrangement and method for reducing the number of processing loops needed to generate an error correction parameter used in the Montgomery method. An initial input to a processing loop is set to a value equal to the modulus, left shifted one register position. Values of the working register are shifted multiple positions during a single loop iteration, and a shifted result is subtracted and compared to zero to determine subsequent contents of the working register.